Telecommunications Cybersecurity and Resilience Act

Senators Mark Warner (D-Virginia) and Ted Cruz (R-Texas)

BACKGROUND

The telecommunications sector is a core component of U.S. critical infrastructure and an increasingly attractive target for sophisticated cyber actors. The Salt Typhoon campaign demonstrated the scale of the threat, with PRC-linked hackers compromising major U.S. telecommunications networks. Salt Typhoon was not an isolated incident, but part of a broader and growing challenge facing communications providers.

THE PROBLEM

Government and the telecommunications industry already share threat information and develop cybersecurity guidance, but those efforts are fragmented and not readily available to the entire industry. Strong cybersecurity practices depend on addressing vulnerabilities across the broader ecosystem, because weaknesses in one part of the network or supply chain create risks elsewhere.

What is missing is a common, telecom sector-specific set of best practices that brings that expertise together and can evolve as threats and technology change. Building on industry's familiarity with security development and threat information sharing, this bill would bring stakeholders – government and private sector – together to develop and maintain effective techniques and practices to secure networks.

THE SOLUTION

The Telecommunications Cybersecurity and Resilience Act creates a voluntary, public-private framework to strengthen telecommunications cybersecurity without imposing new federal mandates. It would:

1. **Create a Telecommunications Cybersecurity Working Group.** Housed within NTIA, the Working Group would bring together telecommunications providers, suppliers, cybersecurity experts, and relevant state, local, and federal agencies.
2. **Require practical, risk-based cybersecurity best practices.** The Working Group would build on existing federal frameworks and threat information while focusing specifically on the telecommunications sector.
3. **Create a voluntary certification process.** Companies could choose to have an independent third-party assessment to certify that they have implemented and maintained the best practices.
4. **Keep pace with changing threats.** The best practices are required to be reviewed at least every two years and following major cyber incidents or significant changes in the threat landscape.
5. **Strengthen the communications networks Americans rely on every day.** By bringing government and industry together to identify and address vulnerabilities across the telecommunications ecosystem, the bill would help make networks more resilient against cyberattacks and other emerging threats.